Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A method of generating kernel audit data comprising:

storing system call parameters or data the system call parameters point to at the beginning of a system call;

~~enabling the generation of audit data when a device driver is opened for read, and halting data generation when the device driver is closed; and~~

and triggering data delivery at the end of a system call path and generating an audit record and depositing the audit record in a circular buffer, wherein the audit record is a tokenized audit record and tokens of the tokenized audit record are either primitive or composed.

2. (currently amended): The method of claim [[1]] 23, wherein for each system call that accesses files, storing related file information.

3. (original): The method of claim 2, wherein related file information includes file owner or group and the file information is stored before any modifications occur that might affect the file information.

4. (currently amended): The method of claim [[1]] 23, wherein system call parameters that include path name parameters are stored with full path name information.

5. (canceled).

6. (currently amended): The method of claim [[1]] 23, further comprising reading audit records from the circular buffer.

7. (original): The method of claim 6, wherein the reading is triggered using a device read call.

8. (currently amended): The method of claim [[1]] 23, comprising maintaining system wide configuration related data structures and setting selection masks based on such structures for specifying data to be delivered.

9. (currently amended): The method of claim [[1]] 23, comprising collecting data in the system call path and formatting the collected data into an audit record.

10. (original): The method of claim 9, wherein the collected data is a token stream.

11. (currently amended): The method of claim [[1]] 23, comprising if the circular buffer is full, then either reading some of the audit records from the circular buffer or dropping new records until space becomes available in the circular buffer.

12. (previously presented): The method of claim 4, comprising maintaining root and current directories while threads are in the middle of system call processing.

13. (original): The method of claim 9, comprising selecting which data to collect before said collecting step.

14. (original): The method of claim 13, wherein said selecting step can be based on process, user, group, filename information and/or time intervals.

15. (currently amended): The method of claim [[1]] 23, further comprising detecting hard link accesses to a critical file.

16. (original): The method of claim 15, comprising maintaining a critical file list for monitoring hard links.

17. (canceled).

18. (previously presented): The method of claim 13, wherein said selecting step can be based on an outcome of system calls including pass, failure or both.

19. (currently amended): The method of claim [[1]] 23, further comprising presenting delivered data to a user space via a device driver in the kernel.

20. (original): The method of claim 13, comprising configuring which system calls are audited by making ioctl() (control) calls on a device driver.

21. (canceled).

22. (canceled).

23. (currently amended) A method of generating kernel audit data comprising:

storing system call parameters or data the system call parameters point to at the beginning of a system call; and

triggering data delivery at the end of the system call and generating an audit record and depositing the audit record in a circular buffer if, based on the success or failure of the system call, auditing of the system call should continue as specified in a post-call selection flag.

24. (new): The method of claim 1, wherein for each system call that accesses files, storing related file information.

25. (new): The method of claim 24, wherein related file information includes file owner or group and the file information is stored before any modifications occur that might affect the file information.

26. (new): The method of claim 1, wherein system call parameters that include path name parameters are stored with full path name information.